

## UNITED STATES DISTRICT COURT

for the  
District of Oregon

FILED 25 FEB '20 08:47 USDC-ORP

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)The person of Julian Muriera, more fully described in  
Attachment A2

Case No.

20-MC--180-A

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The person of Julian Muriera, more fully described in Attachment A2.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2251(a), (e)	Sexual exploitation of a child, attempted sexual exploitation of a child
18 USC 2252(a)(1), (a)(2)	Transportation and distribution of child pornography
18 USC 2252A(a)(5)(B)	Possessing/accessing with intent to view child pornography

The application is based on these facts:

See the attached affidavit of FBI Special Agent Rebecka E. Brown.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Rebecka E. Brown, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Feb. 25, 2020



Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge

Printed name and title

**ATTACHMENT A2**

**Description of Person to be Searched**

The person of Julian Muriera, a white male born March XX, 1983, described as being approximately 5'10" tall and weighing approximately 280 pounds, with brown eyes and black hair.



**ATTACHMENT B****Items to be Searched For, Seized, and Examined**

The following records, documents, and items that constitute contraband and evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2251 (a) and (e), 2252A(a)(2), or 2252A(a)(5)(B).

1. **Records, Documents, and Visual Depictions:**

- a. Any and all records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings that are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;
- d. Any and all records, documents, or materials that include offers to transmit, through interstate commerce by any means (including by computer or smartphone), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;
- e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the

transmission, through interstate commerce (including by computer or smartphone), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, identities assumed for the purposes of communication on the Internet, and Internet search terms or other online inquiries or downloads. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, or live-streaming child pornography, including chat logs, call logs, text messages, instant messages, address book or contact list entries, digital images sent or received, and the like.

i. All records and information regarding the telephone call number of any cellular telephone, and other identifying numbers associated with cellular telephones, computers, or other digital or mobile devices.

j. GPS or other location information for any mobile devices.

2. **Digital Evidence:**

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband or

evidence, fruits, or instrumentalities of such crimes, including central processing units; laptop, notebook, or tablet computers; smartphones; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store contraband or evidence, fruits, or instrumentalities of such crimes;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband, or evidence, fruits, or instrumentalities of such crimes;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;



- f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;
- g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and
- h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

As used herein, the terms "records," "documents," "programs," "applications," or "materials" include records, documents, programs, applications, or materials created, modified, or stored in any form.

#### **Search Procedure**

In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

- a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing

the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and herein.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of

time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data



device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

STATE OF OREGON                    )  
   ) ss.                   AFFIDAVIT OF REBECKA E. BROWN  
 County of Multnomah            )

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Rebecka E. Brown, being duly sworn, hereby depose and state as follows:

**Introduction**

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately eleven years. I am currently assigned to the FBI Portland Field Office's Violent Crimes Against Children squad. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I completed a 21-week course of instruction at the FBI Academy in Quantico, Virginia, which consisted of specialized training in investigating a range of criminal violations. I acquired knowledge and information about crimes from many sources, including formal and informal training, other law enforcement officers and investigators, informants, persons who I have interviewed, and my participation in numerous investigations. I have investigated matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of 18 U.S.C. §§ 2251, 2252A, and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and Task Force Officers from Portland and Hillsboro, Oregon. The CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer or other device.

2. I submit this affidavit in support of applications for warrants to search the premises located at 2974 SE Columbus Avenue, Hillsboro, Oregon 97123 (SUBJECT

PREMISES), further described in Attachment A1, and the person of JULIAN MURIERA, a white male approximately 5'10" in height, weighing approximately 280 pounds, having brown eyes and black hair, and having a date of birth of March XX, 1993, further described in Attachment A2, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) and (e) (prohibiting the production or attempted production of child pornography), 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (prohibiting the distribution and receipt of child pornography, and attempts to do so), and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (prohibiting possessing or accessing with the intent to view child pornography, or attempts to do so). As set forth below, I have probable cause to believe that such items, further described in Attachment B, are currently located at the SUBJECT PREMISES or on MURIERA's person.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

#### **Applicable Law**

4. a. 18 U.S.C. §§ 2251(a) and (e) make it unlawful to knowingly employ, use, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction or transmitting a live visual depiction of such conduct, if the defendant knows or has reason to know the visual depiction will be transported or transmitted

using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or if the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or to attempt to do so.

b. 18 U.S.C. § 2252A(a)(1) makes it unlawful to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) make it unlawful to knowingly receive or distribute child pornography using any means or facility of interstate or foreign commerce, or that has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or to attempt to do so.

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) make it unlawful to knowingly possess or attempt to possess or access or attempt to access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term “child pornography” is defined in 18 U.S.C. § 2256(8).

#### **Background on Computers and Child Pornography**

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers

with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

6. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can upload images or video clips directly from a digital camera or device to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs and networks. Collectors and distributors of child



pornography also use online resources such as “cloud” storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user’s computer.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in “bookmarked” files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces in the computer’s web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

11. Files are transferred between computers, or between a computer and an online data storage service, by reference to an Internet Protocol (IP) address. The IP address is assigned by a user’s Internet Service Provider, and functions much like a telephone number, making it possible for data to be transferred between computers. An IP address can be statically assigned, meaning it is permanently assigned to a particular user and does not change from one Internet session to another. An IP address may also be dynamically assigned, meaning that a different

number may be assigned to a particular user during each Internet session. Internet Service Providers typically log the subscriber to whom a particular IP address is assigned at a particular time.

12. “Cloud” storage is a model of online networked storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centers. Users who wish to store data online buy or lease storage capacity from the hosting company. Once a cloud storage account is established, a user can securely store files or data objects online in the account.

13. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

14. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices through the use of forensic

tools. Indeed, the very nature of the electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.

**Production and Possession of Child Pornography**

15. Based on training and experience, I know individuals involved in the production of child pornography often store pornographic images and videos for their personal review. These explicit images are capable of being stored on a wide variety of digital devices, cellular telephones. Additionally, individuals involved in the production of child pornography often keep pornographic images for distribution, particularly to trade with other individuals involved in the exploitation of children. This trading is often done via the Internet, and through mobile applications including the Kik instant messaging application. Since MURIERA is suspected to be involved in the attempted production of child pornography, and since he used the Kik instant messaging application during the commission of that offense, I believe digital devices, including cellular telephones, found on MURIERA’s person, may contain images and/or videos of child pornography.

16. Those who distribute and collect child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, and typically retain those materials for many years.

17. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close

by, usually at the collector's residence or in their vehicle, to enable the collector to view the collection, which is highly valued.

18. Child pornography collectors and/or distributors also may correspond with and/or meet others to share information and materials; are rarely able to completely destroy correspondence from other child pornography distributors/collectors; conceal correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

19. Individuals involved in the trade of child pornography often use specialized software to conceal the existence of evidence and/or destroy said evidence. There are a variety of different programs that an individual can use to accomplish these objectives, many of which are free. Additionally, child pornographers have been known to store child pornography in unconventional locations on a computer. Often, these files and folders have been renamed in an attempt to mislead investigators.

20. Often, collectors of child pornography will download and store images and communications of children they know or with whom they have communicated. These images many not necessarily be pornographic or obscene in nature, however they are often used for the collectors' sexual gratification.

#### **Background on Kik Messenger**

21. Kik Messenger is a free, Internet-based texting and messaging application for mobile devices. The application is available on most iOS, Android, and Windows smartphone operating systems. Kik Messenger uses a smartphone's data plan or Wi-Fi to transmit and

receive messages. Kik Messenger also allows users to share photos, videos, mobile web pages and other content with other Kik Messenger users, either individually, or in groups. Kik Messenger requires users to register a username and provide an e-mail address, but does not verify the accuracy of a user's registration information.

### **Mobile Communication Devices**

22. I know from training and experience that modern digital devices such as cellular telephones, tablets, and other communication devices are extremely portable. With the advancements in processing power and storage capacity, many of these devices operate similar to stand alone "desktop" type computers. Application developments, communication capabilities and portability have made these devices an indispensable part of everyday life. Persons who have these devices, particularly cellular telephone type platforms, typically keep them on their persons or in other readily available locations. The inherent portability of modern digital devices combined with evidence to believe MURIERA accessed his Kik account on a mobile device from multiple locations give me probable cause to believe that the items referenced in Attachment B could be located on MURIERA's person or within the SUBJECT PREMISES.

### **Statement of Probable Cause**

23. In April 2019, an FBI online covert employee (OCE) was online in an undercover capacity using a cellular device located at the FBI Resident Agency in Fort Wayne, Indiana. The OCE posted numerous online bulletin messages on specific social media forums that the OCE knows are websites frequented by individuals who have a sexual interest in children. The OCE purported to have a 14-year-old step-daughter with whom he was sexually active. One social media platform used by the OCE was Kik.



24. On April 4, 2019, an individual using the Kik screen name “De Teal” and the Kik username “headquest420” sent a personal message to the OCE on Kik. During the online conversations, which lasted from April 4, 2019, to approximately May 9, 2019, “headquest420” expressed interest in watching a live stream on Kik of the OCE engaging in sexual activity with the OCE’s daughter. “headquest420” also sent the OCE an image of a prepubescent girl with her vagina exposed and the text, “just so you know I’m not a cop lmao.” Based on my training and experience, the female in the image appeared to approximately three to five years old. The acronym “lmao” stands for “laughing my ass off.”

25. Over the course of the online conversations, “headquest420” expressed a sexual interest in young children multiple times. Specifically, “headquest420” sent messages to the OCE saying:

“Mine is of my 15 year old neighbor.” *[In this conversation, De Teal was referring to the individual he purportedly had physical access to.]*

“I love it when lolis are into anal...its safer that way haha.” *[I understand “loli” to be a slang term for a girl who is very young and who comes from an elementary school background. “Loli” is also known to mean “a precociously seductive girl.”]*

“She has a really nice ass for a 14 year old. Can I see a face pic so I can umm [sic] all over it. How young do you likem [sic], I prefer 14.”

26. Throughout the duration of the online conversations, “headquest420” provided a list of sexual acts either he wanted to perform or wanted the OCE to perform with the OCE’s daughter via livestream video. Specifically, “headquest420” sent messages to the OCE saying:

“Then I want you to cum in her mouth but she doesn’t swallow it but spits it all back on your dick for her to lick it off and when you are hard again your cock going in her ass. In missionary position so I can see her Pussy. And your gonna spread her push while you fuck her ass. You gonna be using your phone?”

“You need to make her squirt. Just so you know that’s gonna be included on Skype chat. So watch some tutorials if you havent before haha.”

“All respect to you. I’d want to fuck her so hard by myself the first day or time at least haha I’m selfish like that then I’ll be willing to share. Fill her ass up with cum. And watch her spread it as it drips out. She go ass to mouth? . . . I’ll probably make you do that.”

27. On April 6, 2019, the OCE and “headquest420” had a video chat session on Kik. The premise of this video chat was for the OCE and his daughter to live stream themselves performing the sexual acts “headquest420” had previously asked to see. “headquest420” showed the OCE his “Fleshlight,” which had also been discussed in online messages with the OCE.<sup>1</sup> “headquest420” then had a sexual conversation with an FBI Confidential Human Source (CHS) posing as the OCE’s daughter. The conversation occurred in the presence of law enforcement officers and included “headquest420” making the following statements to the CHS:

“...have you ever done ass to mouth?... I will have you do it today then.”

“What’s your favorite (sexual position)? Do you like it when he cums in your ass?”

28. During the video call, law enforcement officers were able to identify “headquest420” as a light skinned male with a round face, wearing a stocking cap style-hat and sunglasses. After the OCE terminated the video call, “headquest420” contacted the OCE on Kik 32 times in the span of one month to reschedule another video call.

29. The FBI issued a subpoena to Kik for records related to user “headquest420.” The information received from Kik included IP address logs showing activity from IP addresses

---

<sup>1</sup> A “Fleshlight” is a brand of masturbation aid for men that consists of a cylindrical tube with an opening that resembles a vagina, anus, or mouth. “headquest420’s” fleshlight was of a mouth.

belonging to Frontier Communications, T-Mobile, and a hospital system in the Portland, Oregon, area during the time periods of interest.

30. The FBI issued a subpoena to Frontier Communications, which reported that the IP addresses around the dates and times of interest were assigned to the SUBJECT PREMISES, with a subscriber name of Katrina Scoppettuolo.

31. According to law enforcement and Oregon Department of Motor Vehicles (DMV) records checks, MURIERA listed the SUBJECT PREMISES as his address. Law enforcement officers also checked employment records for MURIERA, which listed the SUBJECT PREMISES as his address. Those same records also showed a personal cell phone number assigned to the T-Mobile cellular network.

32. The FBI also issued a subpoena to T-Mobile for subscriber information for MURIERA's telephone number. T-Mobile reported the customer's name as "Julian Neal" and the subscriber's name as "Lynda Neal."

33. The FBI learned that MURIERA is employed at Pacific Office Automation. They informed the FBI that the hospital system whose IP address showed up on MURIERA's Kik account is their client, and that MURIERA would have had reason to be at the hospital system during his course of business. MURIERA's timesheet confirmed that he worked on the days the hospital's IP address was used to access MURIERA's Kik account.

34. FBI Fort Wayne located a Facebook profile in the name of JULIAN MURIERA that included photographs of a person who matched MURIERA's DMV photograph. MURIERA was Facebook friends with two Facebook profiles in the name Katrina Scoppettuolo, as well as a Facebook profile in the name of Patty Scoppettuolo.

35. On May 9, 2019, the OCE and “headquest420” conducted a second video call on Kik. The CHS was also present for the call. FBI’s Portland Division conducted physical surveillance on the SUBJECT PREMISES around the timeframe of the planned video call. Neither MURIERA nor his vehicle were seen near the SUBJECT PREMISES during the call. During this second video call, law enforcement officers recognized “headquest420” as the same individual from the first video call. “headquest420” had on similar sunglasses and a similar stocking cap. In the Kik messages that immediately preceded the call, “headquest420” stated, “wish I had my flesh light.” During the video call, “headquest420” made additional sexual statements to the CHS that were similar to ones made in the prior video call and during prior text chats with the OCE, including asking the CHS her “favorite position” and if she “liked swallowing cum.” During this second video call, “headquest420” also briefly removed his sunglasses, allowing law enforcement officers to identify him as MURIERA. The video call was then terminated by the OCE.

36. The FBI issued another subpoena to Kik for user “headquest420” for the time period surrounding the second video call. Kik provided records that showed IP activity from T-Mobile IP address 172.58.41.140. MURIERA’s time cards show he was on a lunch break during the time of the video call. The IP activity on the “headquest420” Kik account that immediately preceded the T-Mobile IP used for the video call were assigned to the same hospital system discovered in the first Kik subpoena return. “headquest420” also had IP activity at the SUBJECT PREMISES on the morning and evening of May 9, 2019.

37. The FBI issued a total of three subpoenas for information pertaining to Kik user “headquest420” covering nearly the entire period between March 9, 2019, and June 18, 2019.

During that time period, Kik records showed user “headquest420” accessed Kik using an iPhone. Kik denotes this on their records using the letters “CIP.” “headquest420” previously installed Kik on an Android device, but Kik records show that Kik was last installed on August 20, 2018. “headquest420” also told the OCE during their chats that he had an iPhone 8 Plus.

38. Furthermore, the FBI served two court orders issued in the Northern District of Indiana to Apple requesting information on Apple ID accounts associated with MURIERA’s telephone number and personal email address, [murierajulian@gmail.com](mailto:murierajulian@gmail.com). Apple records showed an Apple ID associated with MURIERA’s gmail account as well as the same telephone number. The Apple ID had a listed address of Colombus Avenue, Hillsboro, Oregon. No address numerics were included in the return. Apple records also showed on May 9, 2019, MURIERA’s Apple ID downloaded an update from the Apple App Store from the same T-Mobile IP address that was used to conduct the second Kik video call.

39. The premises at 2974 SW Columbus Avenue, Hillsboro, Oregon 97123 are described as a two-story detached structure, blue and tan in color with a brown roof and a red/orange front door. The numbers “2974” are affixed to the left side of the porch column as you are facing the front door. The garage and driveway are accessed from the rear of the structure.

#### **Search and Seizure of Digital Data**

40. The application for the residential warrant seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.



41. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

42. Because it appears that at least one other person resides at the premises, it is possible that the premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the requested warrants would permit the seizure and review of those items as well.

#### **Examination of Data Storage Devices**

43. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

44. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, is often essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data

that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

45. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

46. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that

represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file.

47. *Contextual Data*

a. In some instances, the computer “writes” to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a “picture” of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer’s operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or

edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, and malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to

exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

### **Search Procedure**

48. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

- a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, “computer personnel,”) if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.
- b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.
- c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.



d. *Apple devices with Apple Touch ID.* Based on the foregoing information, I believe MURIERA will have at least one Apple brand device such as an iPhone on his person or at the SUBJECT PREMISES

1. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

2. If a user enables Touch ID on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) at the bottom center of the device. In my training and experience, users of devices that offer Touch ID often enable it because it is a more convenient way to unlock the device than entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

3. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in

8 hours and the passcode or password has not been entered in 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) unsuccessful attempts to unlock the device via Touch ID are made.

4. If Touch ID enabled devices are found during the search, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by the requested warrant. Attempting to unlock the device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices.

5. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area without

any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the SUBJECT PREMISES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

6. Although I do not know which of a given user's ten fingerprints is capable of unlocking a particular device, based upon my training and experience, I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the Premises or person as described above within the five attempts permitted by the Touch ID, the device will require entry of a password or passcode before it can be unlocked.

7. Therefore, I request the Court authorize law enforcement to press the fingers, including thumbs, of individuals found at the SUBJECT PREMISES to the Touch ID sensor of device(s) found at the Premises for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by the requested warrant. I also request that the Court authorize law enforcement to press MURIERA's fingers or thumbs to the Touch ID sensor of any Touch ID-enabled device found on MURIERA's person or in his vehicle.

e. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that

they believe should be seized (e.g. evidence of other crimes), they will seek an additional warrant.

f. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

g. Law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of the execution of the warrant. If, after the initial search, law enforcement personnel determine that an original device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of the chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether the original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

h. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

i. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device, and will seal any image of the device, absent further authorization from the Court.

#### **Data to be Seized**

49. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing



equipment, modems, routers, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data, and;

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the

device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies; bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

50. The government has made no prior efforts in other judicial fora to obtain the evidence sought in this warrant.

#### **Retention of Image**

51. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

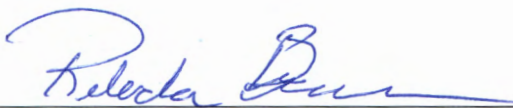
#### **Inventory and Return**

52. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

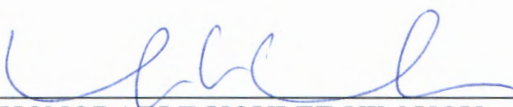
**Conclusion**

53. Based on the foregoing, I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251 (a) and (e) and 18 U.S.C. §§ 2252A(a)(1), (a)(2), (a)(5)(B), (b)(1), and (b)(2) exist on computers and communication devices including any cellular telephones concealed on JULIAN MURIERA's person or in the SUBJECT PREMISES. I therefore request that the Court issue warrants allowing searches of the SUBJECT PREMISES and MURIERA's person, described in Attachments A1 and A2, for the items listed in Attachment B, and the seizure and examination of any such items found.

54. This affidavit, the accompanying applications, and the requested search warrants were all reviewed by Assistant United States Attorney (AUSA) Gary Sussman prior to being submitted to the Court. AUSA Sussman advised me that in his opinion, the affidavit and applications are legally and factually sufficient to establish probable cause to support the issuance of the requested warrants.

  
 \_\_\_\_\_  
 Rebecka E. Brown  
 Special Agent  
 Federal Bureau of Investigation

Subscribed and sworn to before me this 25<sup>th</sup> day of February 2020.

  
 \_\_\_\_\_  
 HONORABLE YOULEE YIM YOU  
 United States Magistrate Judge